Chapter 6
Sample Seven-Step Approach for Implementing a Security Management Process

Introduction

This chapter describes a sample seven-step approach that could be used to implement a security management process in your organization and includes help for addressing security-related requirements of Meaningful Use for the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs. The Meaningful Use requirements for privacy and security (discussed in Chapter 5) are grounded in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. This approach does not cover all the requirements of Meaningful Use and the HIPAA Rules, but following this approach may help you fulfill your compliance responsibilities. This is a sample approach for security management, although occasionally we note related privacy activities.

How to Get Started on Security

Before you start, ask your local Regional Extension Center (REC)[78] where you can get help. In addition:

- Check the Office of the National Coordinator for Health Information Technology (ONC) Health IT Privacy and Security Resources web page.[79]
- Review the Office for Civil Rights (OCR) Security Rule Guidance Material.[80]
- Look at the OCR audit protocols.[81]
- Let your EHR developer(s) know that health information security is one of your major goals in adopting an EHR.
- Check with your membership associations to see if they have training resource lists or suggestions.

[78] http://healthit.gov/rec
[79] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
[80] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
[81] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

- Check to see if your local community college[82] offers any applicable training.
- Discuss with your practice staff, and any other partners you have, how they can help you fulfill your HIPAA Rules responsibilities.

To implement a security management process in your organization, an organized approach to privacy and security is necessary (see Step 2 later in this chapter).

The security management process standard is a requirement in the HIPAA Security Rule. Conducting a risk analysis is one of the requirements that provides instructions to implement the security management process standard. ONC worked with OCR to create a Security Risk Assessment (SRA) Tool[83] to help guide health care providers (from small practices) through the risk assessment process. Use of this tool is not required by the HIPAA Security Rule but is meant to provide helpful assistance.

Before discussing the sample seven-step approach to help providers implement a security management process, one clarification must be emphasized. The scope of a risk analysis for the EHR Incentive Programs security requirements is much narrower than the scope of a risk analysis for the HIPAA Security Rule security management process standard.

The risk analysis requirement in the HIPAA Security Rule is much more expansive. It requires you to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic Protected Health Information (ePHI) that an organization creates, receives, maintains, or transmits — not just the ePHI maintained in Certified EHR Technology (CEHRT). This includes ePHI in other electronic systems and all forms of electronic media, such as hard drives, floppy disks, compact discs (CDs), digital video discs (DVDs), smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media.[84] In addition, you will need to periodically review your risk analysis to assess whether changes in your environment necessitate updates to your security measures.

Under the HIPAA Security Rule, the frequency of reviews will vary among providers. Some providers may perform these reviews annually or as needed depending on circumstances of their environment. Under the EHR Incentive Programs, the reviews are required for each EHR reporting period. For Eligible Professionals (EPs), the EHR reporting period will be 90 days or a full calendar year, depending on the provider's year of participation in the program.

[82] http://www.healthit.gov/policy-researchers-implementers/community-college-consortia
[83] http://healthit.gov/providers-professionals/security-risk-assessment-tool
[84] It's not just the ePHI in EHRs but also in practice management systems, claim processing systems, billing, patient flow (bed management), care and case management, document scanning, clinical portals, and dozens of other ancillary systems that don't meet the definition of CEHRT.

Sample Seven-Step Approach for Implementing a Security Management Process

The sample seven steps which will be discussed here are:

Step 1: Lead Your Culture, Select Your Team, and Learn
Step 2: Document Your Process, Findings, and Actions
Step 3: Review Existing Security of ePHI (Perform Security Risk Analysis)
Step 4: Develop an Action Plan
Step 5: Manage and Mitigate Risks
Step 6: Attest for Meaningful Use Security-Related Objective
Step 7: Monitor, Audit, and Update Security on an Ongoing Basis

Step 1: Lead Your Culture, Select Your Team, and Learn

Your leadership — especially your emphasis on the importance of protecting patient information — is vital to your practice's privacy and security activities. Your commitment to an organized plan and approach to integrating privacy and security into your practice is important.

This first step in your seven-step approach presents six actions that you should take to set the stage for implementing an effective security management process for your organization. Each of these six actions is discussed below.

1A. Designate a Security Officer(s)
1B. Discuss HIPAA Security Requirements with Your EHR Developer
1C. Consider Using a Qualified Professional to Assist with Your Security Risk Analysis
1D. Use Tools to Preview Your Security Risk Analysis
1E. Refresh Your Knowledge Base of the HIPAA Rules
1F. Promote a Culture of Protecting Patient Privacy and Securing Patient Information

Step 1A: Designate a Security Officer(s)

Your security officer will be responsible for developing and maintaining your security practices to meet HIPAA requirements. This person could be part of your EHR adoption team and should be able to work effectively with others.

A security officer is responsible for protecting your patients' ePHI from unauthorized access by working effectively with others to safeguard patient information. At various times, the officer will

need to coordinate with your privacy officer (if a different person), practice manager, information technology (IT) administrator or consultant, your EHR developer, and legal counsel.

When you designate your officer(s), be sure to:

- Record all officer assignments in a permanent documentation file (this file should focus on HIPAA compliance efforts), even if you are the officer(s).
- Discuss your expectations for the officer and his/her accountability. Note that you, as a Covered Entity (CE), retain ultimate responsibility for HIPAA compliance.
- Enable your designated officer(s) to develop a full understanding of the HIPAA Rules so they can succeed in their roles. For example, allow them time to participate in privacy and security presentations, seminars, and webinars and to read and review the Final Rules and the analysis and summaries on the ONC Health IT Privacy and Security Resources web page,[85] including the helpful OCR audit protocols.[86] Have them use the ONC Cybersecure training games[87] as a useful training tool.

Step 1B: Discuss HIPAA Security Requirements with Your EHR Developer

As you prepare for the security risk analysis, meet with your EHR developer to understand how your system can be implemented in a manner consistent with the HIPAA requirements and those for demonstrating Stage 1 and Stage 2 Meaningful Use (see Chapters 4 and 5).

- Before you purchase an EHR, perform your due diligence by discussing and confirming privacy and security compliance requirements and product capabilities. Refer to the listing of CEHRT developers[88] as you proceed.
- If you have implemented an EHR, confirm your practice's understanding of the overall functions that your EHR product offers and then assess your current security settings.
- You would want to make sure that the EHR system can be configured to your policies and procedures and that the EHR will sign a Business Associate Agreement (BAA) that reflects your expectations. Confirm any planned additional capabilities that you need or that your EHR developer is responsible for providing, especially if any are required to demonstrate Meaningful Use. Ask the developer for its pricing for training staff on those functions, developing relevant policies and procedures, and correcting security-setting deficiencies in the EHR system.

Step 1C: Consider Using a Qualified Professional to Assist with Your Security Risk Analysis

Your security risk analysis must be conducted in a manner consistent with the HIPAA Security Rule, or you will lack the information necessary to effectively protect ePHI. Note that doing the analysis in-house

[85] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
[86] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
[87] http://www.healthit.gov/providers-professionals/privacy-security-training-games
[88] http://oncchpl.force.com/ehrcert?q=chpl

may require an upfront investment of your time and a staff member's time to understand and address electronic information security issues and the HIPAA Security Rule.

- A qualified professional's expertise and focused attention can often yield quicker and more reliable results than if your staff does an in-house risk analysis in a piecemeal process spread over several months. Certification (see box at right) can be one indicator of qualifications. The professional will suggest ways to mitigate risks so you can avoid the need to research and evaluate options yourself.
- Talk to several sources of potential assistance. If you contract with a professional, ONC recommends that you use a professional who has relevant certification and direct experience tailoring a risk analysis to medical practices with a similar size and complexity as yours.

You are still ultimately responsible for the security risk analysis even if you hire a professional for this activity. Further, the security risk analysis will require your direct oversight and ongoing involvement.

The security risk analysis process is an opportunity to learn as much as possible about health information security. See Step 3 in this chapter for more discussion about security risk analyses.

Certification in Health Information Security

Some professionals have a certification in health information. For example, the Healthcare Information and Management Systems Society (HIMSS) and the American Health Information Management Association (AHIMA) are two organizations that offer certifications upon successful completion of an exam.

Certified in Healthcare Privacy and Security (CHPS)

This credential is designated to professionals who are responsible for safeguarding patient information. This credential signifies expertise in planning, executing, and administering privacy and security protection programs in health care organizations and competence in a specialized skill set in the privacy and security aspects of health information management.

Certified Professional in Healthcare Information and Management Systems (CPHIMS)

CPHIMS is a professional certification program for health care information and management systems professionals.

Step 1D: Use Tools to Preview Your Security Risk Analysis

Have your security officer or security risk professional consultant use tools available on the ONC and OCR websites to get a preliminary sense of potential shortcomings in how your practice protects patient information. A single listing of areas of focus or a checklist does not fulfill the security risk analysis requirement, but these types of tools will help everyone get ready for needed

improvements. Keep the results as part of your documentation (see Step 2). Consider the SRA Tool[89] and OCR Guidance on Risk Analysis[90] for more thorough guidance in evaluating your level of risk.

Step 1E: Refresh Your Knowledge Base of the HIPAA Rules

Learn about the HIPAA Rules, state laws, and other privacy and security requirements that also require compliance.

Step 1F: Promote a Culture of Protecting Patient Privacy and Securing Patient Information

Privacy and security are best achieved when the overall atmosphere in your office emphasizes confidentiality and protecting of patient information. Culture sets the tone that will:

- Consistently communicate your expectations that all members of your workforce protect patients' health information
- Guide your workforce's efforts to comply with, implement, and enforce your privacy and security policies and procedures
- Remind staff why securing patient information is important to patients and the medical practice

Step 2: Document Your Process, Findings, and Actions

Documentation of a risk analysis and HIPAA-related policies, procedures, reports, and activities is a requirement under the HIPAA Security Rule. Also, the Centers for Medicare and Medicaid Services (CMS) advise all providers who attest for the EHR Incentive Programs to retain all relevant records that support attestation.

Documentation shows how you did the security risk analysis and implemented safeguards to address the risks identified in your risk analysis. (See the box at right for additional items to include in your documentation folder.)

Over time, your security documentation folder will become a tool that helps your security procedures be more

Examples of Records to Retain

Contents should include, but not be limited to, the following:

- Your policies and procedures
- Completed security checklists
- Training materials presented to staff and volunteers; any associated certificates of completion
- Updated BA agreements
- Security risk analysis report
- EHR audit logs that show both utilization of security features and efforts to monitor users' actions
- Risk management action plan or other documentation (that shows appropriate safeguards are in place throughout your organization), implementation timetables, and implementation notes
- Security incident and breach information

[89] http://healthit.gov/providers-professionals/security-risk-assessment-tool
[90] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

efficient. Your workforce will be able to reference this master file of security findings, decisions, and actions. Further, the information will be more accurate than if your workforce tries to reconstruct past decisions and actions. These records will be essential if you are ever audited for compliance with the HIPAA Rules[91] or an EHR Incentive Program.

Step 3: Review Existing Security of ePHI (Perform Security Risk Analysis)

The risk analysis process assesses potential threats and vulnerabilities to the confidentiality, integrity, and availability of ePHI. The findings from this analysis inform your risk mitigation strategy.

Before you start, these recommended resources can provide guidance on your security risk analysis:

- OCR's Guidance on Risk Analysis Requirements under the HIPAA Security Rule[92]
- OCR Security Rule Frequently Asked Questions (FAQs)[93]
- SRA Tool,[94] which helps small practices conduct an extensive, systematic risk analysis
- National Institute of Standards and Technology (NIST) HIPAA Security Rule Toolkit[95]

If you want additional support, a security risk professional can plan and implement this analysis, but you will need to oversee the process. Some commercial security risk analysis products are available, but before you buy, seek out an independent review from a health information security expert.

Your first comprehensive security risk analysis should follow a systematic approach that covers all security risks. It should:

- Identify where ePHI exists in your practice and how it is created, received, maintained, and transmitted, including in your EHR. Types of risks to the ePHI maintained in your EHR will vary depending on whether your EHR is based in your office or hosted on the Internet (e.g., cloud-based or Application Service Provider).
- Identify potential threats and vulnerabilities to ePHI. Potential threats include human threats, such as cyber-attack, theft, or workforce member error; natural threats, such as earthquake,

Tips for a Better Security Risk Analysis

- Educate staff about the iterative and ongoing nature of the security risk analysis process.
- Make security a high priority in your workplace culture.
- Have an action plan that clearly assigns responsibilities for each risk analysis component.
- Involve your EHR developer in the process.
- Ensure that the risk analysis is specific to your situation.

91 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html
92 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
93 http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/index.html
94 http://www.healthit.gov/providers-professionals/security-risk-assessment-tool
95 http://scap.nist.gov/hipaa/

fire, or tornado; and environmental threats, such as pollution or power loss. Vulnerabilities are flaws or weaknesses that if exploited by a threat could result in a security incident or a violation of policies and procedures.

- Identify risks and their associated levels (e.g., high, medium, low). This is done by assessing the likelihood that threats will exploit vulnerabilities under the safeguards currently in place and by assessing the potential impacts to confidentiality, integrity, and availability of ePHI.

A risk analysis can produce results that may fall into "gray" areas. However, you will be able to see where you are meeting, not meeting, or exceeding HIPAA requirements at a given point in time.

Security Risks in Office-Based EHRs vs. Internet-Hosted EHRs

All types of EHRs outperform paper medical records when it comes to providing better access to and use of ePHI. On the other hand, EHRs also introduce new risks to ePHI. The mix of security risks is affected, in part, by the type of EHR hosting you have: office-based (local host) or Internet-hosted (remote host). Table 2 offers a few examples of different risks associated with office-based vs. Internet-hosted EHRs.

Table 2: Examples of Potential Information Security Risks with Different Types of EHR Hosts

Host Type	Risk	Examples of Mitigation Steps
Office-Based EHRs	Natural disaster could greatly disrupt the availability of, and even destroy, ePHI.	Always store routine backups offsite.
Office-Based EHRs	You directly control the security settings.	Regardless of your practice size, follow best practices on policies and procedures about access to ePHI. For example, use password controls and automatic logout features.
Office-Based EHRs	The security features on your office-based EHR may not be as up-to-date and sophisticated as an Internet-hosted EHR.	Maintain ongoing communication with your EHR developer about new features and their criticality to the security of the EHR.
Office-Based EHRs	When public and private information security requirements change, you have to figure out how to update your EHR and work out any bugs.	Routinely monitor for changes in federal, state, or private-sector information security requirements and adjust settings as needed.
Internet-Hosted (Cloud-Based) EHRs	You are more dependent on the reliability of your Internet connection. Your data may be stored outside the U.S., and other countries may have different health information privacy and security laws that may apply to such offshore data.	Confirm that your EHR host follows U.S. security standards and requirements.
Internet-Hosted (Cloud-Based) EHRs	The developer may control many security settings.	The adequacy of these settings may be hard to assess, but ask for specific information.
Internet-Hosted (Cloud-Based) EHRs	In the future, the developer might request extra fees to update your EHR for compliance as federal, state, and private-sector information security requirements evolve.	Ensure your EHR stays compliant. Before you buy, it is OK to ask your developer about fees it may charge for security updates.

Step 4: Develop an Action Plan

Using the results from your risk analysis, discuss and develop an action plan to mitigate the identified risks. Your action plan is informed by your risk analysis and should focus on high priority threats and vulnerabilities. Take advantage of the flexibility that the HIPAA Security Rule provides, which allows you to achieve compliance while taking into account the characteristics of your organization and its

environment. It is important that your security plan is feasible and affordable for your practice. Often, basic security measures can be highly effective and affordable (see box below).

Action Plan Components

The plan should have five components:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational standards
- Policies and procedures

These components correspond with the security components specified in the table on the next page. Table 3 briefly outlines each component and provides examples.

Low-Cost, Highly Effective Safeguards

- Say "no" to staff requests to take home laptops containing unencrypted ePHI.
- Remove hard drives from old computers before you get rid of them.
- Do not email ePHI unless you know the data is encrypted.
- Make sure your server is in a room accessible only to authorized staff, and keep the door locked.
- Make sure the entire office understands that passwords should not be shared or easy to guess.
- Notify your office staff that you are required to monitor their access randomly.
- Maintain a working fire extinguisher in case of fire.
- Check your EHR server often for viruses and malware.

Table 3: Five Security Components for Risk Management

Security Component	Examples of Vulnerabilities	Examples of Security Mitigation Strategies
Administrative Safeguards	• No security officer is designated. • Workforce is not trained or is unaware of privacy and security issues. • Periodic security assessment and	• Security officer is designated and publicized. • Workforce training begins at hire and is conducted on a regular and frequent basis. • Security risk analysis is performed periodically and when a change occurs in the practice or the technology.
Physical Safeguards	• Facility has insufficient locks and other barriers to patient data access. • Computer equipment is easily accessible by the public. • Portable devices are not tracked or not locked up when not in use.	• Building alarm systems are installed. • Offices are locked. • Screens are shielded from secondary viewers.
Technical Safeguards	• Poor controls allow inappropriate access to EHR. • Audit logs are not used enough to monitor users and other EHR activities. • No measures are in place to keep electronic patient data from improper changes. • No contingency plan exists. • Electronic exchanges of patient information are not encrypted or otherwise secured.	• Secure user IDs, passwords, and appropriate role-based access are used. • Routine audits of access and changes to EHR are conducted. • Anti-hacking and anti-malware software is installed. • Contingency plans and data backup plans are in place. • Data is encrypted.
Organizational Standards	• No breach notification and associated policies exist. • Business Associate (BA) agreements have not been updated in several years.	• Regular reviews of agreements are conducted and updates made accordingly.
Policies and Procedures	• Generic written policies and procedures to ensure HIPAA security compliance were purchased but not followed. • The manager performs ad hoc security measures.	• Written policies and procedures are implemented and staff is trained. • Security team conducts monthly review of user activities. • Routine updates are made to document security measures.

For any single risk, a combination of safeguards may be necessary because there are multiple potential vulnerabilities. For example, ensuring appropriate and continuous access to patient information may require something as simple as a physical safeguard of adding a power surge protection strip, putting the server in a locked room, and being meticulous about backups. Your action plan should have multiple combinations of the five required components. Although the steps are sequential, the security components are interrelated.

Learn more about these requirements through the HIPAA Security Rule Educational Paper Series,[96] the ONC Cybersecurity web pages,[97] and the Cybersecure training games.[98]

Process for Developing the Plan

Your security officer (see Step 1A) will need to convene the team to develop the security action plan. Begin by identifying the simple actions that can reduce the greatest risks.

If your staff is unsure how specific HIPAA requirements might apply to your specific practice, review OCR Security Rule Guidance[99] or other materials on ONC's Health IT Privacy and Security Resources web page.[100] Ask your security risk professional or legal counsel for help as needed.

Once the plan is written, your designated security team should meet periodically to coordinate actions, work through unexpected snags, and track progress. Reward your team as it achieves milestones. Understand that you will not be able to eliminate risk, but you will be able to lower it by implementing safeguards that reduce risk and vulnerabilities. More about implementing the action plan is in Step 5 below.

Step 5: Manage and Mitigate Risks

Once you have an action plan, follow it to reduce security risks and better protect ePHI. This step has four parts, each of which is discussed below.

Key Questions to Ask as You Plan

Who has keys to your practice?

Establish and follow a policy regarding keys and passwords. Ensure that access keys are returned before employees or contractors leave your practice. If any former employees and contractors have keys, change the locks. Do not forget about "virtual" keys like administrator accounts to your EHR or database — be sure to change these passwords periodically.

Where, when, and how often do you back up? Do you have at least one backup kept offsite? Can your data be recovered from the backups?

Periodically test your backup system to confirm you can retrieve your data backups when needed.

What is your contingency/ disaster plan when/if your server crashes and you cannot directly recover data?

Always maintain developer documentation that provides contact information and the serial numbers of your server and other hardware and software used, etc. Keep one copy offsite in a secure place.

[96] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
[97] http://www.healthit.gov/providers-professionals/cybersecurity-shared-responsibility
[98] http://www.healthit.gov/providers-professionals/privacy-security-training-games
[99] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
[100] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

5A. Implement Your Action Plan (which includes using applicable EHR security settings and updating your HIPAA-related policies and procedures)
5B. Prevent Breaches by Educating and Training Your Workforce
5C. Communicate with Patients
5D. Update Your BA Contracts

Throughout this process, continue your efforts to build a culture that values patients' health information and actively protects it. One easy way is to give your staff time to play ONC's Cybersecure training games.[101] The games are a fun and engaging way to provide answers to many of the everyday questions around safeguarding PHI.

Step 5A: Implement Your Action Plan

The goal of following your security risk action plan is to protect patient ePHI through ongoing efforts to identify, assess, and manage risks. As discussed in Step 4, your action plan, regardless of how it is organized, should address all five HIPAA security components:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational standards
- Policies and procedures

This section focuses on technical safeguards and policies and procedures. Chapter 4 and Chapter 6 (Steps 1, 4, and 5D) provide additional information about these five components.

Information Security Settings in Your EHR

If an EHR is certified,[102] it has a package of core technical security functions, such as the ability to authenticate users with valid accounts. However:

- Use of CEHRT does not mean that your practice is "HIPAA compliant."
- Certification does not guarantee performance or reliability of security functions in CEHRT, especially if you turn off functions that are important to Privacy and Security Rule compliance.
- The security functions of the CEHRT may be "off," or the settings could be at a suboptimal level — both can create vulnerabilities.

[101] http://www.healthit.gov/providers-professionals/privacy-security-training-games
[102] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification.html

It is vital that your practice learns about the security settings in your EHR, and your assigned EHR administrator(s) must have access to these settings. Your Health Information Exchange (HIE) may have specific requirements for security settings.

Your risk analysis should specifically examine the adequacy of your EHR security safeguards as your system transmits, stores, and allows modifications to ePHI.

Information Security: Encryption

Per the HIPAA Security Rule, a CE, such as a health care provider, must use encryption if, after implementing its security management process, it determines that encryption is a reasonable and appropriate safeguard in its practice environment to safeguard the confidentiality, integrity, and availability of ePHI.

Need assistance with appropriately configuring your EHR security features? In addition to working with an information security expert, gather information from sources such as:

- ONC's Health IT Privacy and Security Resources web page[103]
- Your EHR developer
- Your state or county medical association

Written Policies and Procedures

With respect to protecting patient information, your policies and procedures guide how your practice operates on a day-to-day basis. Your medical practice policies and procedures should accomplish the following, at minimum:

- Establish protocols for all five security components (administrative, physical, and technical safeguards; organizational standards; and policies and procedures).
- Commit to a HIPAA training program for all new staff when they are hired and on a regular basis for the entire workforce.
- Instruct your workforce on what to do when something happens that impairs the availability, integrity, or confidentiality of ePHI. (Sometimes these instructions are labeled as "incident response" or "breach notification and management" plans.)
- Specify a sanction policy for violations of the Privacy, Security, or Breach Notification Rules or your policies and procedures. Your sanction policy must be applied consistently as written.
- Detail enforcement, starting with the use of your EHR security audit logs to monitor access, use, and disclosure of ePHI.
- Specify the need for written agreements with BAs that detail their specific responsibility to comply with privacy and security.

[103] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

As you make the updates, retain outdated policies and procedures in your security documentation folder as described in Step 2.

Once your written policies and procedures are in place, the HIPAA Rules require that you do the following:

- Train your workforce (see Step 5B) on what is required and how to implement the policies and procedures. HIPAA requires that your workforce be specifically trained on these policies and procedures, including breach notification. Your workforce will need periodic refresher training on new aspects of your security program.
- Confirm that you have identified all your BAs. Contact them and confirm through written agreements that they understand their responsibilities to carry out HIPAA Rules requirements and to inform you of any breaches.
- Consistently apply your policies and procedures when unauthorized access to PHI occurs. Whenever a member of your workforce does not comply with your policies and procedures, he or she must be sanctioned. You must have a sanctions policy in place to ensure all members of the workforce are treated fairly. Document your actions.
- Periodically review your policies and procedures to make sure they are current and your practice adheres to them.
- Update your policies and procedures when changes in your internal or external environment create new risks.
- Retain policies and procedures in your documentation folder for at least six years after you have updated or replaced them (see Step 2). State and private-sector requirements may specify a longer time period for retention.

Step 5B: Prevent Breaches by Educating and Training Your Workforce

Workforce education and training — plus a culture that values patients' privacy — are a necessary part of risk management. All of your workforce members — employees, volunteers, trainees, and contractors supporting your office — need to know how to safeguard patient information in your practice. Your training program should prepare your workforce to carry out:

- Their roles and responsibilities in safeguarding patients' health information and complying with the HIPAA Rules
- Your HIPAA-related policies
- Your procedures, including processes to monitor security and steps for breach notifications

Your workforce may need focused training to develop the requisite skills to perform the steps you require. ONC's Cybersecure training games[104] and mobile device training videos[105] are highly recommended resources.

Reinforce workforce training with reminders. Above all, lead by example by adhering to your policies and procedures.

Frequency of Workforce Training

Your practice must educate and train individual workforce members at the time each person is hired or contracted. Industry best practices suggest that the entire workforce should be trained at least once every year and any time your practice changes its policies or procedures, systems, location, infrastructure, etc. It is particularly important that your workforce be trained on how to respond immediately to any potential security incidents or an unauthorized disclosure of ePHI because these situations may be breaches.

Making Protecting Patient Information Part of Your Routine

Deliberately create a culture that emphasizes PHI confidentiality. You can do this in a number of ways, which include:

- Speaking often about the importance of trust in the patient-provider relationship. Remind your workforce that patients expect your practice to be a good steward of their health information.
- Continually reminding staff to safeguard patient confidentiality and the security of ePHI.
- Making sure your staff has a copy of your policies and procedures for easy reference. Remind them to comply with those policies and procedures.
- Addressing staff questions, and getting outside resources to help if you feel you need additional expertise with message delivery.
- Reassessing each workforce member's job functions and enabling him/her to access only the minimum necessary health information as appropriate.

Step 5C: Communicate with Patients

Your patients may be concerned about the confidentiality and security of their health information in an EHR. Don't wait for them to ask. Instead, provide them with information about EHRs, especially the

[104] http://www.healthit.gov/providers-professionals/privacy-security-training-games
[105] http://www.healthit.gov/providers-professionals/worried-about-using-mobile-device-work-heres-what-do-video

benefits EHRs can bring to them as patients. Reassure patients that you have a system to proactively protect the privacy and security of their health information. Your staff should be able to speak to the confidentiality and security of your EHR as well.

To preserve good patient relations, follow your policies and procedures for communicating with patients and caregivers if a breach of unencrypted ePHI ever occurs. As explained in Chapter 7, OCR and most state attorneys general strictly enforce breach procedures.

A multi-faceted communications plan will help you avert patient concerns about EHRs and privacy.

- Inform patients that you place a priority on maintaining the security and confidentiality of their health information. ONC and other federal agencies have developed consumer education handouts[106] that you may want to use or adapt.
- Address patients' individual health information rights, which include the right to access or obtain a copy of their electronic health record in an electronic form.
- Educate patients about how their health information is used and may be shared outside your practice. In some cases, depending on state law and the nature of information you are sharing, you may need to obtain a patient's permission (consent or authorization) prior to exchanging his/her health information.
- Notify affected patients and caregivers when a breach of unsecured PHI has occurred, in accordance with your updated policies and procedures.

Patient relations on security issues should be an integral part of your overall patient engagement strategy.[107]

Consumer communications should be culturally appropriate. Consider the various languages, communication needs, and trust levels of different patient populations. If a particular group has some distrust of the medical establishment, take extra steps to reassure them that you are safeguarding their information.

Be prepared to discuss and answer the questions that concerned patients and their caregivers may have. For ideas, visit the ONC Health IT Privacy and Security Resources web page,[108] which provides other materials for you and your patients.

[106] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
[107] http://www.healthit.gov/patients-families/protecting-your-privacy-security and http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf
[108] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

Fulfill Your Responsibilities for Patients' Health Information Rights[109]

In the future, expect more patients to ask how you handle their electronic health information. More patients will ask for their medical records, and some will want changes made in their records. As part of the HIPAA Rules and Stage 2 Meaningful Use, you must respond to these patient requests. In particular:

- Patients can request copies of and access to their PHI in paper or electronic format, including from your EHR. Meaningful Use Core Objectives indicate that such ePHI held in the EHR should be made available to patients, upon request, **within four business days** of it being available to the provider (see Chapter 3).
- Patients can request corrections and amendments to the PHI in their records; this is called a "right to amend" and has always been part of the HIPAA Rules. Now Stage 2 Meaningful Use Objective 9 **requires you to respond to patients' requests to amend their ePHI that is in your EHR**.
- Under the Privacy Rule, a patient, or another person on a patient's behalf, can ask his/her provider to restrict submission of his/her PHI to the patient's health plan **when the patient has paid in full** for the health care service or item — and the provider must honor that request.

To prepare for patient requests, ask your EHR developer about ways to use your system to help you fulfill individual patient rights. For example, confirm what EHR capabilities are currently available and when additional capabilities will be available (such as amendments to and copies of their ePHI). Your developer or other expert consultant may also be able to assist you in implementing these features both in your EHR and your practice workflow. Ask your EHR developer to provide step-by-step instructions or best practice guidelines that include screen shots on how to perform these actions.

Once you have established a process and procedure on how to provide patients with a copy of their medical information from your EHR, develop an understanding of and procedures for what to do when patients ask you to modify or to amend their health information, restrict disclosure, or obtain a report about prior disclosures. (See Chapter 2.)

Online Communications with Patients

If you plan to interact with patients via online platforms (e.g., email, texting, a patient portal for your EHR, or social media), you must meet the Security Rule and Meaningful Use standards for the secure messaging of ePHI.

[109] OCR's patient access memo may be a helpful resource regarding patients' health information rights: http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/righttoaccessmemo.pdf

Remember that a provider who is emailing and texting patients and/or other providers is creating a security risk for the ePHI unless the transmission is encrypted. See the sidebar "Email and Texting" in Chapter 4 and visit the ONC website for information about the risks of emailing via mobile devices[110] and texting health information.[111] Read the Stage 2 EP Meaningful Use Core and Menu Measures Table of Contents.[112] If you have continued questions, obtain guidance from appropriate legal counsel.

Step 5D: Update Your BA Contracts

Be sure to update all your BA agreements to comply with the HIPAA Privacy, Security, and Breach Notification Rules.[113] (Refer to Chapter 2 for a refresher on the definition of a BA.) Such agreements should require your BAs to:

- Fully comply with relevant safeguards for PHI that they get from your practice
- Train their workforce
- Adhere to additional requirements for patient rights and breach notification

OCR offers sample BA contract provisions.[114]

Developers Supporting Health Information Exchange Are Often Considered BAs

Developers that support your practices through cloud computing/storage or secure physical storage facilities are most likely among your practice's BAs.

Step 6: Attest for Meaningful Use Security-Related Objective

The EHR Incentive Programs provide incentive payments to EPs as they demonstrate adoption, implementation, upgrading, and meaningful use of CEHRT. These Meaningful Use Programs are designed to support providers with the health information technology (health IT) transition and instill the use of EHRs to improve the quality, safety, and efficiency of patient health care.

Providers can register for the EHR Incentive Programs[115] anytime, but attesting requires you to have met the Meaningful Use requirements for an EHR reporting period. So, only attest for an EHR Incentive Program after you have fulfilled the security risk analysis requirement and have documented your efforts. Specifically, you should not attest until you have conducted your security risk analysis (or reassessment) *and* corrected any deficiencies identified during the risk analysis. Document these changes.

[110] http://www.healthit.gov/providers-professionals/faqs/can-you-use-email-send-health-information-using-your-mobile-device
[111] http://www.healthit.gov/providers-professionals/faqs/can-you-use-texting-communicate-health-information-even-if-it-another-p
[112] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2_MeaningfulUseSpecSheet_TableContents_EPs.pdf
[113] Modifications to the Rules expand the types of entities considered BAs and place more obligations on BAs to strictly follow the HIPAA Security Rule.
[114] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
[115] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/RegistrationandAttestation.html

When you attest[116] to Meaningful Use, it is a legal statement that you have met specific standards, including that you protect electronic health information. Providers participating in the EHR Incentive Programs can be audited.

If you attest prior to actually meeting the Meaningful Use security requirement, it is possible you could increase your business liability for violating federal law and making a false claim. Consult with appropriate legal counsel for further guidance. From this perspective, consider implementing multiple security measures prior to attesting. The priority would be to mitigate high-impact and high-likelihood risks.

Step 7: Monitor, Audit, and Update Security on an Ongoing Basis

Step 7 relates to the HIPAA Security Rule requirements that you have audit controls in place and have the capability to audit. HIPAA uses the term "audit" in two ways. In the first context, audit is what you *do* to monitor the adequacy and effectiveness of your security infrastructure and make needed changes.

- Have your security officer, IT administrator, and EHR developer work together so your system's monitoring/audit functions are active and configured to your needs. They may want you to:
    - Decide whether you will conduct the audits in-house, use an information security consultant, or have a combination of the two
    - Determine what to audit and how the audit process will occur
    - Identify trigger indicators — or signs that ePHI could have been compromised and further investigation is needed
    - Establish a schedule for routine audits and guidelines for random audits

In the second context, audit refers to an effort to *examine* what happened. This means your EHR must be set up to maintain retrospective documentation (i.e., an "audit log") on who, what, when, where, and how your patients' ePHI has been accessed. Such audits (i.e., the auditing process, which would examine logs) are required security technical capabilities that would be part of your Stage 1 and 2 Meaningful Use demonstrations. These capabilities include auditable events and tamper resistance, audit logs, access control and authorizations, automatic logoff, and emergency access (see Stage 2 Meaningful Use Core Measure 9[117] for more description).

Your audit controls and capabilities should be scaled to your practice's size. For example, your certified EHR has a function to generate audit logs. This means it can record when, where (e.g., which laptop), and how ePHI is accessed; by whom; what the individual did; and for what purposes. Your EHR can then produce reports using these data. Such audit logs are useful tools for both holding your workforce

[116] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/RegistrationandAttestation.html
[117] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/Stage2_EPCore_9_ProtectElectronicHealthInfo.pdf

accountable for protecting ePHI and for learning about unexpected or improper modifications to patient information.

Medical Record Retention

As you know, state law requires you to store medical records for a specified number of years. Your obligations and the length of time to maintain patient medical records recorded in an EHR are usually also a matter of your state's medical record retention laws. These laws are often found in a state's licensing laws.

If one of your BAs is an HIE, your written agreement with the HIE should require it to return or securely dispose of the ePHI it creates, receives, maintains, or transmits on behalf of your practice (the CE).

This Guide is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers and professionals to seek expert advice when evaluating the use of this Guide.